International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 6, Issue 2, Apr 2016, 1-10

A NOVEL IMAGE WATERMARKING SYSTEM UTILIZING HMM IN WAVELET DOMAIN

B. GOPI[1] & T. SUDHA[2]

[1]*Research Scholar, Department of CS, Vikrama Simhapuri University, Nellore, Andhra Pradesh, India*

[2]*Professor & HOD, Department of CS, Sri Padmavati Mahila Viswavidhyalayam, Tirupati, Andhra Pradesh, India*

ABSTRACT

Achieving high capacity, sufficient imperceptibility and enough robustness is crucial for a good image watermarking scheme. In this paper a novel image watermarking algorithm is proposed which uses Taylor series approximated locally optimum test (TSLOT) detector, Hidden Markov Model (HMM) in wavelet domain using bi-orthogonal 9/7 wavelet. TSLOT based HMM in wavelet domain is established to handle the question of unavailability of exact embedding strength in the receiver due to informed embedding. Then based on the TSLOT detector new HMM-based spherical codes are built to afford an effective balance among robustness and distortion. The process of informed embedding is expressed as an optimization problem under the robustness and distortion restrictions and the genetic algorithm (GA) is then employed to solve this problem. Simulation results demonstrate that the proposed informed watermarking algorithm has high robustness against common attacks in signal processing.

KEYWORDS: Informed Watermarking, Hidden Morkov Model, Wavelet, GA

Received: Jan 28, 2016; **Accepted:** Feb 10, 2016; **Published:** Feb 19, 2016; **Paper Id.:** IJCSEITRAPR20161

Original Article

INTRODUCTION

The most important issue in digital watermarking community is robust watermarking, which aims at achieving imperceptibility, robustness and high capacity simultaneously [1]. However, these three goals are contrary to each other, and consequently a worthy design is necessary to attain a suitable compromise between them. Digital watermarking systems are narrowly associated to the problem of communication with side information at the encoder. The pioneer research by Costa [2] shows that, for a power constrained input ‘x’ and a channel with additive white Gaussian noise (AWGN) and additive white Gaussian state sequence, the capacity is the same as that of AWGN channel with only ‘z’ when the state ‘s’ is known to the encoder. This result inspires the development of tough and high-capacity watermarking systems by considering the watermark as x and the host signal as in the Costa’s model. The realization of this hint leads to an informed watermarking technique, which sheds much vision on the strategy of high capacity and robust watermarking systems and therefore turn into a field of extensive research [3]–[4]. Works shows from the theoretic [5]–[6] and practical [3][7] point of views that informed watermarking can attain the best performance in robustness and capacity by adapting to the interference bring together by host signals.

The informed watermarking systems in the literatures can be divided into two groups, namely, 1) the quantization index modulation (QIM) proposed by Chen and Wornell [4] and 2) the spread spectrum (SS)-based informed watermarking systems [8]. The QIM takes the lattice code as the codebook and uses the quantization to perform embedding and decoding. In [9], Erez and Zamir proved that lattice code can attain the capacity of

log(1+SNR)/2 for AWGN channel when the code length reaches maximum. This group of systems can attain comparatively high capacity with low computational complexity while being generally exposed to amplitude scaling attack.

In recent times, numerous methodologies exploiting the inserted pilot signal and exploiting the rational dither modulation have been devised to improve the robustness against scaling attack. In [10], Malvar*et al.* proposed an improved spread spectrum watermarking system (ISS). By adapting to the host, as the source of interference, ISS attains substantial progress in terms of robustness performance. Two related systems were proposed in [8], which use informed coding and informed embedding. In informed coding, the message is first associated with a co-set comprising more than one code-words, and the ideal code-word is then preferred from the associated co-set to characterize the message, where the correlation detector is usually adopted. In informed embedding, the selected code-word is tailored, according to both the host signal and the restraints of robustness and distortion, so as to put the watermarked signal into the detection region of the selected code-word. By utilizing spherical codes lying on the surface of sphere with radius one, both [8] and [11] have good performances against scaling attack.

The system in [11] was assessed through Monte Carlo simulation, while a practical informed watermarking system with superior robustness performance was demonstrated in [8]. The computational complexity of the latter algorithm, however, is relatively high, which partly comes from the fact that the system uses the trellis code with a long code-word length to attain a high robustness. Informed watermarking typically entails an adequate number of code-words in each co-set when random codes are utilized, so that it can find with high probability a suitable code-word to adapt to the informed host interference. However, the minimum distance between co-sets d_{min} tends to decrease as the number of code-words growths, which usually leads to degraded robustness against non-informed channel attacks. Miller *et al.*'s system in [8] employs dirty-paper trellis code with a long code-word length to tackle the robustness issue, where each path and thus each message order are coded with multiple vectors [8].

HIDDEN MORKOV MODEL

The Hidden Markov Model (HMM) is a commanding statistical tool for modeling generative sequences that can be described by a primary process generating an observable order. Andrei Markov offered his name to the mathematical theory of Markov processes in the early twentieth century, but it was Baum and his colleagues that established the theory of HMMs in the 1960s.

Markov Processes

Figure 1 shows an illustration of a Markov process. The model presented describes a simple model for a stock market index. The model has three states, Bear, Bull and Even, and three index observations down, up and unchanged. The model is a finite state mechanism, with probabilistic transitions among states from each other. Given a sequence of observations, example: up-down-down we can easily verify that the state sequence that formed those observations was: Bull-Bear-Bear, and the probability of the sequence is the product of the transitions, in this case $0.2 \times 0.3 \times 0.3$.

Hidden Markov Models

Figure 2 shows an illustration of how the preceding model can be stretched into a HMM. The new model now permits all observation symbols to be emitted from each state with a finite probability. This modification makes the model much more expressive and able to well characterize our insight, in this case, that a bull market would have equally good

days and bad days, but there would be more good ones. The key difference is that now if we have the observation sequence up-down-down then we cannot say exactly what state sequence formed these observations and thus the state sequence is 'hidden'. We can then compute the probability that the model produced the sequence, as well as which state sequence was most likely to have created the observations.

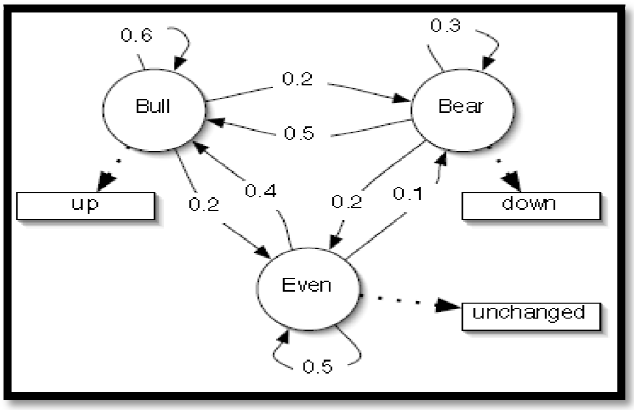

Figure 1: Markov Process [21]

The definition of a HMM is as follows:

$$\lambda = (A, B, \pi) \tag{1}$$

S is state alphabet set, and V is the observation alphabet set:

$$S = (s_1, s_2, \cdot\cdot\cdot, s_N) \tag{2}$$

$$V = (v_1, v_2, \cdot\cdot\cdot, v_M) \tag{3}$$

We define Q to be a fixed state sequence of length T, and corresponding observations O:

$$Q = q_1, q_2, \cdot\cdot\cdot, q_T \tag{4}$$

$$O = o_1, o_2, \cdot\cdot\cdot, o_T \tag{5}$$

A is a transition array which stores the probability of state j following state i. Note the state transition probabilities are not dependent on time:

$$A = [a_{ij}]\ ,\ a_{ij} = P(q_t = sj\ |q_{t-1} = s_i)\ . \tag{6}$$

B is the observation array which stores the probability of observation k being produced from the state j, independent of t:

$$B = [b_i(k)]\ ,\ b_i(k) = P(x_t = v_k|q_t = s_i)\ . \tag{7}$$

π is the initial probability array:

$$\pi = [\pi_i]\ ,\ \pi_i = P(q_1 = s_i) \tag{8}$$

Two assumptions are made by the model. The first, called the Markov assumption, states that the current state is reliant on only on the previous state, this represents the memory of the model:

$$P(q_t|q_1^{t-1}) = P(q_t|q_{t-1}) \tag{9}$$

The independence assumption states that the output observation at time t is dependent only on the current state, it is independent of previous observations and states:

$$P(o_t|o_1^{t-1}, q_t^1) = P(o_t|q_t) \tag{10}$$

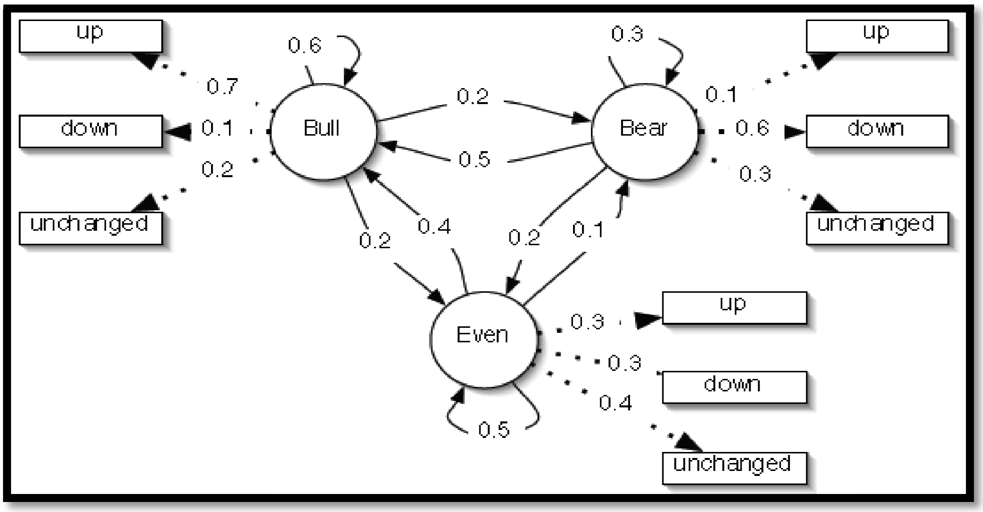

Figure 2: Hidden Markov Model [21]

INFORMED WATERMARKING

In previous work [12], it was shown that high robustness can be achieved if the watermark signal is embedded in the perceptually most significant components of the host signal. In second generation watermarking systems, info about the original signal is exploited explicitly by the encoder. The watermarking process is assumed as a channel coding problem, which needs a precise characterization of the channel. Second generation watermarking systems do not consider the host signal as noise to the watermark signal.

Watermarking Channel

In watermarking applications, the audio signal constitutes the channel for communication of the watermark data. Defining the channel capacity is vital and, in the case of digital music, is a tough problem that comprises subjective considerations such as the maximum distortion that can be bring together to the music without creating noticeable artifacts. Psychoacoustic models can be utilized to find out non-perceptible components and the watermark energy is concentrated in unexploited redundancy of the audio signal. Hence watermarking algorithms are in direct competition with lossy audio encoders such as MPEG-1 layers.

In addition, large intervention and deformation of the channel may result from coding, signal processing operations or malevolent attacks, and may extremely narrow the capacity. As long as the bit-rate of the embedded data does not surpass the channel capacity, Shannon has revealed that it is possible to attain consistent transmission of the watermark [13].

Blind Watermarking

In blind watermarking systems, decoding is attained without alternative to the original signal. Therefore, if w(t) = s(t)- sw(t) is the watermark bring together in the original audio signal, s(t), to produce the watermarked audio signal, sw(t),

blind recovery of the embedded information requires w(t) to be uncorrelated with s(t). In [25—27], a dither modulation system was engaged to modulate a digital watermark signal into images. In this approach, the noise bring together by a quantizer is dither-modulated exploiting a digital pseudo-random watermarking map. If the size of the codebook is adequately large, the noise signal bring together by the quantizer is about white and uncorrelated with the audio signal, which promises blind recovery. A high degree of robustness can be attained by intensification of the modulated quantization noise. Though, invisibility of the mark cannot be assured. In addition, high performance perceptual coders or malevolent attackers will tend to filter out uncorrelated noise and abolish the concert of such systems. In [14], elements of perceptual models for the human visual system are bring together to select the DFT components most relevant to the human visual system, which are next utilized to carry the mark. This results in the colouring of the quantization noise according to the signal spectrum, which defines a tradeoff between robustness and awareness of the watermark.

PROPOSED ALGORITHM

In this section, the proposed HMM-based informed watermarking algorithm, which comprises the message embedding and extraction processes as shown in figure 3 was presented. For each vector tree T_i, the embedding process contains two stages, i.e., choosing the representative code-word M_{bi} with respect to the input message bit (b_i = 0,1) and utilizing the GA-based informed embedding to find the optimal embedding strength vector A_{opt_bi} for M_{bi}. The extraction process employs the TSLOT detector to recover the message.

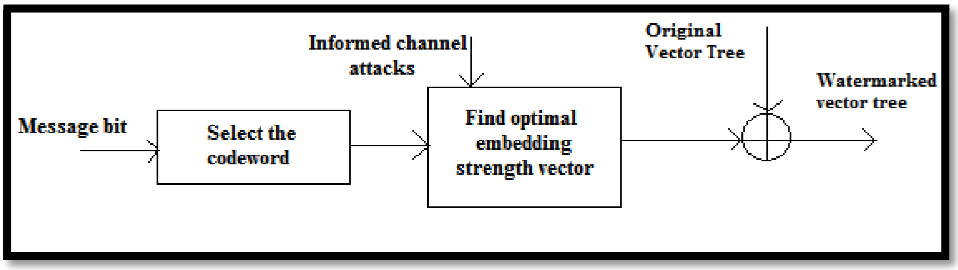

Figure 3: Embedding Process

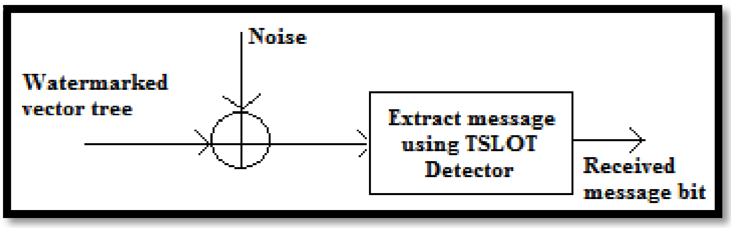

Figure 4: Extraction Process

Let the host signal I(x,y) be an image of size L_1 x L_2. Suppose that the message to be embedded b consists of random bits. The embedding of secrete data in the proposed HMM-based informed watermarking can be described as follows.

- Decompose the host image I(x,y) with the bi-orthogonal 9/7 wavelet (which is considered in this work) into a three-level wavelet pyramid, and use the coarsest two levels to construct (L_1L2/64 number of) vector trees as shown in figure 5.

- To attain high robustness, insert one bit into one vector tree, which in turn need generating the message b of ($L_1L2/64$ number of) random bits. Permute b with the secret key say K so as to enhance the secrecy. Assign one permuted bit b_i (b_i=0,1) to each vector tree T_i(i=1,.., $L_1L2/64$) , which clues to an information rate of 1/64 bit/pixel.
- Relate the given message bit b_i to its respective code-word M_{bi}.
- Decide the optimal strength vector A_{opt_bi} for M_{bi} through informed embedding, which is framed as a GA-based optimization problem and embed (A_{opt_bi}o M_{bi}) into T_i via the rule $Y_i = T_i + A_{opt_bi}$o M_{bi}.
- After completing embedding of all message bits into their respective vector trees via Steps 3) & 4), perform the inverse wavelet transformation to obtain the watermarked image $I^w(x,y)$.

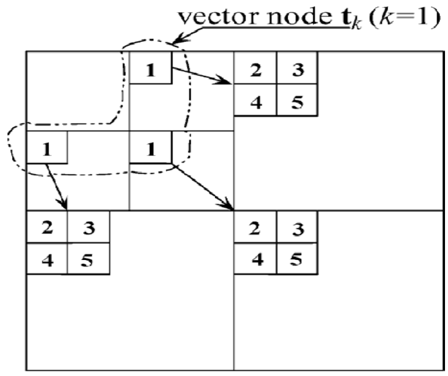

Figure 5: Vector Trees in Wavelet Decomposed Image Data

The extraction process is shown in figure 4. For a given vector tree T_i(i=1,.., $L_1L2/64$), the two embedding strength vectors A_0 and A_1 (corresponding to b_i=0 and 1, respectively) are controlled so that the subsequent code-words (A_0 º M_0) and (A_1 º M_1) are positioned at the neighborhood of M_0 and M_1, which can be well detected by the TSLOT detector. Upon receiving the possibly attacked watermarked image $I^r(x,y)$, the TSLOT detector is utilized to recover the message from $I^r(x,y)$, which is listed as follows.

- Decompose the received image into a three-level wavelet pyramid with the bi-orthogonal 9/7 wavelet and then build the vector trees utilizing the coarsest two levels.
- For each vector tree, use the TSLOT detector to find a code-word with the maximum TSLOT value, called $M_{bir}\epsilon$ { M_0,M_1} (b_i^r = 0,1).
- Use the respective co-set index (0 or 1) of M_{bir} as the mined message bit $b_i^r \epsilon$ {0,1}.
- After handling all vector trees, rearrange the extracted bit stream with the key K to recover the message sequence b^r.

SIMULATION RESULTS

In this section the simulation results of the proposed algorithm are presented. The following figure shows the GUI utilized in MATLAB. The input image utilized as host image is first applied to histogram modification. Then the locations where the secrete data has to be embedded is calculated by utilizing HMM. Then the secrete data is embedded in the wavelet decomposed data of host image as explained in the previous section. The below figure shows the GUI after

execution. Along with no attack case, a number of attacks are also considered. The PSNR obtained is shown in the table below with different attacks.

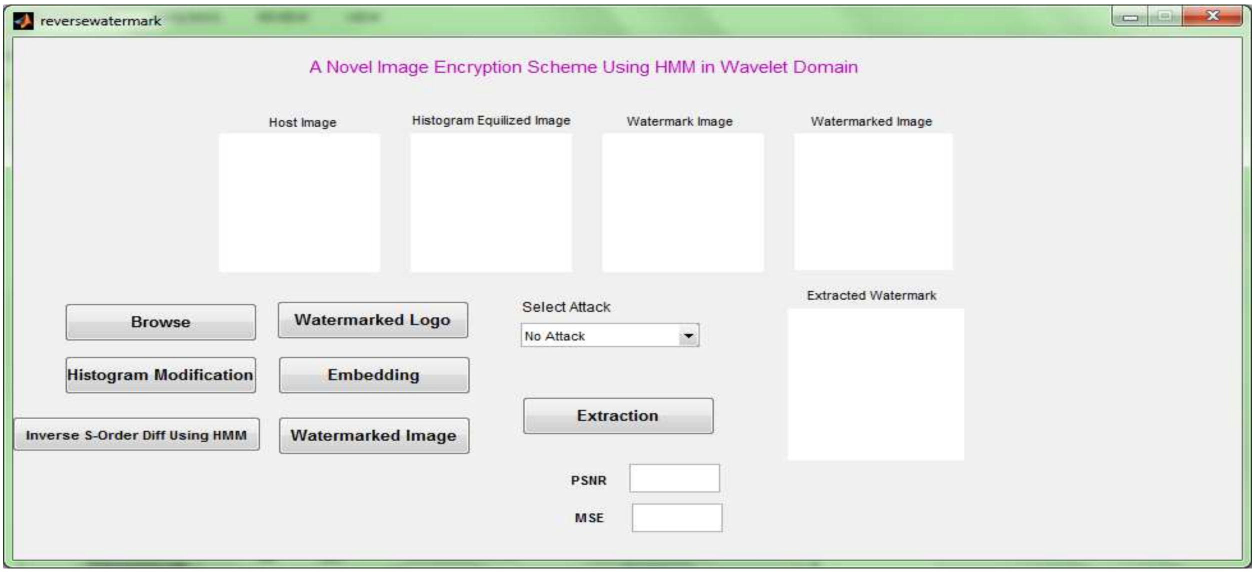

Figure 6: GUI before the Execution

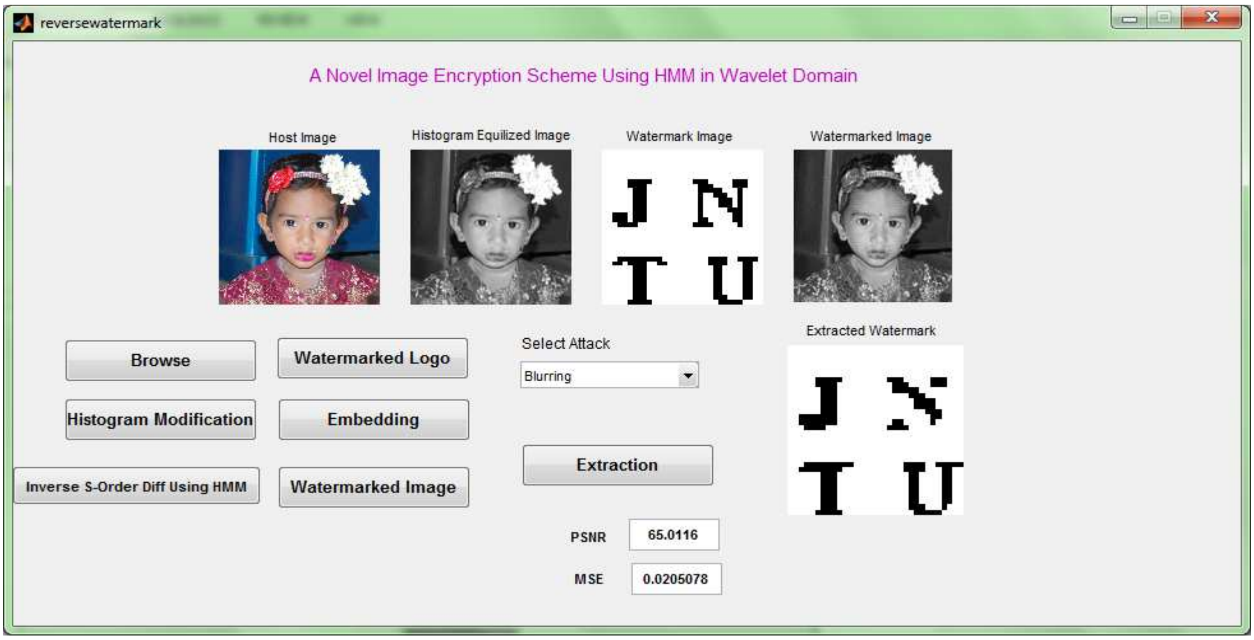

Figure 7: GUI before the Execution

Table 1: Performance of the Proposed Technique with different Attacks

	MSE	PSNR
No Attack	0	inf
Blurring	0.02	65.01
Gaussian	0.08	59.14
Salt & Pepper	0.036	62.55
Compression	0.046	61.42
Poisson	0.97	48.25
Speckle	0.07	59.66

CONCLUSIONS

In this paper a new HMM based image watermarking technique is developed utilizing HMM in wavelet domain. The host image is first decomposed by biorthogonal wavelet. Utilizing the coarsest two levels to construct $L_1L2/64$ vector trees are constructed. After finding the optimal location the secrete data is embedded bit by bit. Then inverse wavelet transform is applied. The PSNR and MSE are calculated between the input image and watermarked image. In the extraction phase, the watermarked image is decomposed by the biorthogonal wavelet. After constructing the vector trees utilizing coarsest two levels, TSLOT detector is utilized to extract the data bit from the vector trees.

REFERENCES

1. *J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking. San Mateo, CA: Morgan Kaufmann, 2001.*
2. *M. H. M. Costa, "Writing on dirty paper," IEEE Trans. Inform. Theory, vol. IT-29, no. 3, pp. 439–441, May 1983.*
3. *I. J. Cox, M. L. Miller, and A. L. McKellips, "Watermarking as communications with side information," Proc. IEEE, vol. 87, no. 7, pp. 1127–1141, Jul. 1999.*
4. *B. Chen and G. W. Wornell, "Quantization index modulation methods: A class of provably good methods for digital watermarking and information embedding," IEEE Trans. Inform. Theory, vol. 47, no. 4, pp. 1423–1443, May 2001.*
5. *P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," in Proc. IEEE Int. Symp. Inform. Theory, Jun. 2000, p. 19.*
6. *P. Moulin, "The role of information theory in watermarking and its application to image watermarking," Signal Process., vol. 81, no. 6, pp. 1121–1139, Jun. 2001.*
7. *J. J. Eggers, J. K. Su, and B. Girod, "A blind watermarking system based on structured codebooks," Proc. Inst. Elec. Eng., Secure Images and Image Authentication, vol. 4, pp. 1–6, Apr. 2000.*
8. *M. L. Miller, G. J. Doerr, and I. J. Cox, "Applying informed coding and embedding to design a robust high capacity, watermark," IEEE Trans. Image Process., vol. 13, no. 6, pp. 792–807, Jun. 2004.*
9. *U. Erez and R. Zamir, "Achieving 0.5 log(1+SNR)/2 over the additive white Gaussian noise channel with lattice encoding and decoding," IEEE Trans. Inform Theory, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.*
10. *H. S. Malvar and A. F. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," IEEE Trans. Signal Process., vol. 51, no. 4, pp. 898–905, Apr. 2003.*
11. *A. Abrardo and M. Barni, "Informed watermarking by means of orthogonal and quasi-orthogonal dirty paper coding," IEEE Trans. Signal Process., vol. 53, no. 2, pp. 824–833, Feb. 2005.*
12. *Huang et. al. Spoken Language Processing, Prentice Hall PTR.*
13. *C. E. Shannon, "A mathematical theory of communication," Bell Syst. Tech. J., v. 27, pp. 379-423, 623- 656, 1948.*
14. *G. C. M. Silvestre and W. J. Dowling, "Embedding data in digital images utilizing CDMA techniques," in Proc of 2000 IEEE Int. Conf. on Image Proc., Vancouver,* Canada, pp. 589-592, v. I, September 10-13, 2000.

AUTHOR'S DETAILS

B. Gopi received Masters in Computer Science and Applications and Masters in Technology from SV University, Tirupati and Acharya Nagarjuna University, Guntur respectively. He worked as Senior Lecturer in the Department of Computer Science and Applications in Sri Karunamayi Institute of Higher Learning, Gudur from 2007 to 2010. Currently heis a full time researchscholarat the Department of Computer Science in Vikrama Simhapuri University, Nellore. Hisresearchinterestsinclude Fractal theory, Image Encryption.

Prof. T Sudha is currently working as Professor and Head of the Department, Dept. of CS in Sri Padmavathi Mahila Viswavidhyalayam, Tirupati. She has held many positions in Sri Padmavathi Mahila Viswavidhyalayam as well as other institutes like Vikrama Simhapuri University, Nellore. She did M.Sc., M.Phil., Ph.D and MS all on Computer Science field. She has published a number of research papers in national and international journals.